

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

Docket No.: 60188-093

PATENT

JC997 U.S. PTO
09/942594
08/31/01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

#3

In re Application of

Teruo AKASHI

Serial No.:

Group Art Unit:

Filed: August 31, 2001

Examiner:

For: LICENSE ISSUING DEVICE/METHOD AND CONTENTS REPRODUCING
DEVICE/METHOD

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Commissioner for Patents
Washington, DC 20231

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicant hereby claims the priority of:

Japanese Patent Application No. 2000-262912,
Filed August 31, 2000

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY


Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:ykg
Date: August 31, 2001
Facsimile: (202) 756-8087

日本国特許庁
JAPAN PATENT OFFICE

60188-093
AUGUST 31, 2001
AKASHI
McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出願年月日

Date of Application:

2000年 8月31日

出願番号

Application Number:

特願2000-262912

出願人

Applicant(s):

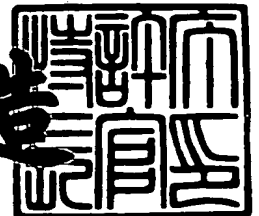
松下電器産業株式会社



2001年 5月31日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3050329

【書類名】 特許願

【整理番号】 2037820034

【提出日】 平成12年 8月31日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 明石 輝夫

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100077931

【弁理士】

【氏名又は名称】 前田 弘

【選任した代理人】

【識別番号】 100094134

【弁理士】

【氏名又は名称】 小山 廣毅

【選任した代理人】

【識別番号】 100110939

【弁理士】

【氏名又は名称】 竹内 宏

【選任した代理人】

【識別番号】 100110940

【弁理士】

【氏名又は名称】 嶋田 高久

【選任した代理人】

【識別番号】 100113262

【弁理士】

【氏名又は名称】 竹内 祐二

【選任した代理人】

【識別番号】 100115059

【弁理士】

【氏名又は名称】 今江 克実

【選任した代理人】

【識別番号】 100115510

【弁理士】

【氏名又は名称】 手島 勝

【選任した代理人】

【識別番号】 100115691

【弁理士】

【氏名又は名称】 藤田 篤史

【手数料の表示】

【予納台帳番号】 014409

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0006010

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ライセンス発行装置、コンテンツ再生装置、ライセンス発行方法、およびコンテンツ再生方法

【特許請求の範囲】

【請求項 1】 自己を一意に識別することができる装置 ID と相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置に、コンテンツの利用を許可するライセンス情報を書き込むライセンス発行装置であって、

利用者が携帯するライセンス記憶装置の正当性を認証する認証手段と、

前記利用者が携帯するライセンス記憶装置が正当なものであると前記認証手段によって認証されたとき、前記利用者によって指定されたコンテンツの利用を許可するライセンス情報を作成する手段と、

前記ライセンス情報作成手段によって作成されたライセンス情報を前記利用者が携帯するライセンス記憶装置の装置 ID を用いて暗号化して、当該暗号化したライセンス情報を前記利用者が携帯するライセンス記憶装置に書き込む第 1 の暗号化手段とを備える

ことを特徴とするライセンス発行装置。

【請求項 2】 請求項 1 に記載のライセンス発行装置において、

前記ライセンス情報は、

前記利用者によって指定されたコンテンツを識別するためのコンテンツ ID を含む

ことを特徴とするライセンス発行装置。

【請求項 3】 請求項 1 に記載のライセンス発行装置において、

前記ライセンス情報は、

前記利用者によって指定されたコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含む

ことを特徴とするライセンス発行装置。

【請求項 4】 請求項 1 に記載のライセンス発行装置において、

前記ライセンス情報は、

前記利用者によって指定されたコンテンツを復号するための復号化鍵を含む

ことを特徴とするライセンス発行装置。

【請求項 5】 請求項 1 に記載のライセンス発行装置において、

前記認証手段は、

前記利用者が携帯するライセンス記憶装置が有する装置鍵を用いて、前記利用者が携帯するライセンス記憶装置の装置 ID を暗号化する第 2 の暗号化手段を含み、

前記第 1 の暗号化手段は、

前記第 2 の暗号化手段によって暗号化された装置 ID を用いて前記ライセンス情報を暗号化して、当該暗号化したライセンス情報を前記利用者が携帯するライセンス記憶装置に書き込む

ことを特徴とするライセンス発行装置。

【請求項 6】 請求項 1 に記載のライセンス発行装置において、

前記ライセンス発行装置は、前記利用者が携帯するライセンス記憶装置にネットワークを介して接続される

ことを特徴とするライセンス発行装置。

【請求項 7】 暗号化されたコンテンツを復号して再生するコンテンツ再生装置であって、

前記コンテンツ再生装置は、

自己を一意に識別することができる装置 ID と相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置の装置 ID を用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものであり、

利用者が携帯するライセンス記憶装置の正当性を認証する認証手段と、

前記利用者が携帯するライセンス記憶装置が正当なものであると前記認証手段によって認証されたとき、前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、当該ライセンス記憶装置の装置 ID を用いて復号する復号手段と、

前記復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する再生手段とを

備える

ことを特徴とするコンテンツ再生装置。

【請求項 8】 請求項 7 に記載のコンテンツ再生装置において、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを復号するための復号化鍵を含むものであり、

前記再生手段は、

前記復号手段によって得られたライセンス情報に含まれる復号化鍵を用いて、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号する

ことを特徴とするコンテンツ再生装置。

【請求項 9】 請求項 7 に記載のコンテンツ再生装置において、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを識別するためのコンテンツ ID を含むものであり、

前記再生手段は、

前記復号手段によって得られたライセンス情報に含まれるコンテンツ ID を用いて、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを取得する

ことを特徴とするコンテンツ再生装置。

【請求項 10】 請求項 7 に記載のコンテンツ再生装置において、

前記コンテンツ再生装置はさらに、

暗号化されたコンテンツを蓄積する手段を備え、

前記再生手段は、

前記復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを前記蓄積手段から取得する

ことを特徴とするコンテンツ再生装置。

【請求項 11】 請求項 7 に記載のコンテンツ再生装置において、

前記再生手段は、

前記復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得することを特徴とするコンテンツ再生装置。

【請求項 1 2】 請求項 7 に記載のコンテンツ再生装置において、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含むものであり、

前記再生手段は、

前記復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件に従って、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生することを特徴とするコンテンツ再生装置。

【請求項 1 3】 請求項 1 2 に記載のコンテンツ再生装置において、

前記コンテンツ再生装置はさらに、

前記復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件を、前記再生手段によるコンテンツの再生に応じて更新するコンテンツ利用条件更新手段と、

前記復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件に代えて前記コンテンツ利用条件更新手段によって更新されたコンテンツ利用条件を含んだ更新後ライセンス情報を生成する手段と、

前記更新後ライセンス情報生成手段によって生成された更新後ライセンス情報を前記利用者が携帯するライセンス記憶装置の装置 ID を用いて暗号化する手段と、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、前記暗号化手段によって暗号化された更新後ライセンス情報に書き換える手段とを備える

ことを特徴とするコンテンツ再生装置。

【請求項 1 4】 暗号化されたコンテンツを復号して再生するコンテンツ再生装置であって、

前記コンテンツ再生装置は、

自己を一意に識別することができる装置 I D と相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置の装置鍵を用いて暗号化された当該ライセンス記憶装置の装置 I D、を用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものであり、

利用者が携帯するライセンス記憶装置の正当性を認証し、当該ライセンス記憶装置が正当であると認証されたとき、当該ライセンス記憶装置の装置鍵を用いて当該ライセンス記憶装置の装置 I D を暗号化して暗号化装置 I D を生成する認証手段と、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、前記認証手段によって生成された暗号化装置 I D を用いて復号する復号手段と、

前記復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する再生手段とを備える

ことを特徴とするコンテンツ再生装置。

【請求項 1 5】 自己を一意に識別することができる装置 I D と相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置に、コンテンツの利用を許可するライセンス情報を書き込むライセンス発行方法であって、

利用者が携帯するライセンス記憶装置の正当性を認証し、

前記利用者が携帯するライセンス記憶装置が正当なものであると認証されたとき、

前記利用者によって指定されたコンテンツの利用を許可するライセンス情報を前記利用者が携帯するライセンス記憶装置の装置 I D を用いて暗号化して、当該暗号化したライセンス情報を前記利用者が携帯するライセンス記憶装置に書き込む

ことを特徴とするライセンス発行方法。

【請求項 1 6】 暗号化されたコンテンツを復号して再生するコンテンツ再生方法であって、

前記コンテンツ再生方法は、

自己を一意に識別することができる装置 I D と相手装置の正当性を認証する機能とを有する携帯可能なライセンス記憶装置の装置 I D を用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものであり、

利用者が携帯するライセンス記憶装置の正当性を認証するステップと、

前記認証ステップにおいて前記利用者が携帯するライセンス記憶装置が正当なものであると認証されたとき、前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、当該ライセンス記憶装置の装置 I D を用いて復号するステップと、

前記復号ステップによって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生するステップとを備える

ことを特徴とするコンテンツ再生方法。

【請求項 1 7】 請求項 1 6 に記載のコンテンツ再生方法において、

前記再生ステップでは、

前記復号ステップによって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得する

ことを特徴とするコンテンツ再生方法。

【請求項 1 8】 請求項 1 6 に記載のコンテンツ再生方法において、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含むものであり、

前記再生ステップでは、

前記復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件に従って、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する

ことを特徴とするコンテンツ再生方法。

【請求項 1 9】 請求項 1 8 に記載のコンテンツ再生方法において、

前記復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件を、前記再生ステップにおけるコンテンツの再生に応じて更新するステップと、

前記復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件に代えて前記更新ステップによって更新されたコンテンツ利用条件を含んだ更新後ライセンス情報を、前記利用者が携帯するライセンス記憶装置の装置 I D を用いて暗号化するステップと、

前記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、前記暗号化ステップによって暗号化された更新後ライセンス情報に書き換えるステップとをさらに備えることを特徴とするコンテンツ再生方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、ライセンス発行装置、コンテンツ再生装置、ライセンス発行方法、およびコンテンツ再生方法に関する。さらに詳しくは、コンテンツと当該コンテンツのライセンスとを分離して提供するコンテンツ提供システムにおけるライセンス発行装置、コンテンツ再生装置、ライセンス発行方法、およびコンテンツ再生方法に関する。

【0 0 0 2】

【従来の技術】

デジタル技術の発達により、ソフトウェアプログラムのみならず、絵画、音楽、映画などの著作物もデジタルデータとして管理され、流通するようになっている。近年ではさらに、ネットワーク技術の著しい進歩により、これらの著作物を、時間と場所を問わず、ネットワークを介して利用者に配布することが可能な環境が整いつつある。

【0 0 0 3】

デジタルデータとしてのこれらのコンテンツは、従来のアナログデータと異な

り、複製を繰り返しても品質が劣化しない。したがって、コンテンツを販売する側としては、流通しているコンテンツが著作権者の許可なく複製されるような不正利用を防止することが不可欠である。この点に関しては、暗号技術の発展がコンテンツのセキュリティレベルの向上に寄与している。暗号化技術としては、暗号化鍵と復号化鍵に同一の鍵を用いる対称暗号の一種であるDESや、暗号化と復号化とで鍵の異なる非対称暗号のRSA暗号などが知られている。

【0004】

コンテンツの不正利用を防ぐ技術の第1の例として、販売しようとするコンテンツの全部または一部をあらかじめ暗号化してそのままでは利用不可能な状態に保護しておき、利用者が保護状態を解除するためのライセンスを購入する、という販売方式がある。この方式では、コンテンツを再生する装置に固有のIDを認識し、配布するライセンスをこのIDを含めて暗号化しておく。そして、再生時に、ライセンスを復号化して取り出したIDと再生装置に固有のIDとを比較して一致した場合にのみ再生を行う。このように、コンテンツを再生できる装置を限定し、不正に複製された装置上での利用を防いでいる。

【0005】

また、第2の例として、ネットワーク上に管理センターを設け、コンテンツの再生時に、ネットワークを介して管理センターに接続し、パスワード等によりあらかじめ登録された利用者の認証を行うという手法がある。

【0006】

【発明が解決しようとする課題】

上述の第1の例においては、コンテンツをライセンスとともに購入した後では、コンテンツを再生できる装置はライセンスを受けた再生装置に限定される。このため、コンテンツが自由に流通するようになっても、そのコンテンツを利用するときには再生装置の制約を受ける。すなわち、特定のコンピュータにライセンスされたプログラムは、そのコンピュータにアクセスしなければ利用できない。家庭の据置型プレーヤにライセンスされた音楽は、外出先の携帯端末では利用できない。携帯型ビデオ再生装置にライセンスされた映画は、家庭内の大画面ディスプレイを備える装置では再生できない。このような種々の不具合が生じる。

【 0 0 0 7 】

また、上述の第 2 の例においては、ネットワークに接続でき、かつ管理センターと通信するための手段が不可欠となる。したがって、このような機能を持たない再生装置での利用は制限される。

【 0 0 0 8 】

【課題を解決するための手段】

この発明の 1 つの局面に従うと、ライセンス発行装置は、携帯可能なライセンス記憶装置に、コンテンツの利用を許可するライセンス情報を書き込むものである。ライセンス記憶装置は、自己を一意に識別することができる装置 ID と相手装置の正当性を認証する機能とを有する。ライセンス発行装置は、認証手段と、ライセンス情報作成手段と、第 1 の暗号化手段とを備える。認証手段は、利用者が携帯するライセンス記憶装置の正当性を認証する。ライセンス情報作成手段は、利用者が携帯するライセンス記憶装置が正当なものであると認証手段によって認証されたとき、利用者によって指定されたコンテンツの利用を許可するライセンス情報を作成する。第 1 の暗号化手段は、ライセンス情報作成手段によって作成されたライセンス情報を利用者が携帯するライセンス記憶装置の装置 ID を用いて暗号化して、当該暗号化したライセンス情報を利用者が携帯するライセンス記憶装置に書き込む。

【 0 0 0 9 】

上記ライセンス発行装置では、利用者が希望するコンテンツのライセンス情報を、携帯可能な独立したハードウェアであるライセンス記憶装置に書き込む。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、ライセンス記憶装置に対応したさまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【 0 0 1 0 】

また、ライセンス情報は、ライセンス記憶装置の装置 ID を用いて暗号化される。これにより、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【 0 0 1 1 】

また、上記ライセンス発行装置は、コンテンツのライセンス情報だけを利用者の携帯するライセンス記憶装置に書き込む。したがって、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、利用者はライセンス記憶装置の記憶容量を気にする必要もない。

【 0 0 1 2 】

また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は1つのライセンス記憶装置でたくさんのコンテンツを利用することができる。

【 0 0 1 3 】

好ましくは、上記ライセンス情報は、利用者によって指定されたコンテンツを識別するためのコンテンツIDを含む。

【 0 0 1 4 】

好ましくは、上記ライセンス情報は、利用者によって指定されたコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含む。

【 0 0 1 5 】

好ましくは、上記ライセンス情報は、利用者によって指定されたコンテンツを復号するための復号化鍵を含む。

【 0 0 1 6 】

好ましくは、上記認証手段は、第2の暗号化手段を含む。第2の暗号化手段は、利用者が携帯するライセンス記憶装置が有する装置鍵を用いて、利用者が携帯するライセンス記憶装置の装置IDを暗号化する。そして、上記第1の暗号化手段は、第2の暗号化手段によって暗号化された装置IDを用いてライセンス情報を暗号化して、当該暗号化したライセンス情報を利用者が携帯するライセンス記憶装置に書き込む。

【 0 0 1 7 】

好ましくは、上記ライセンス発行装置は、利用者が携帯するライセンス記憶装置にネットワークを介して接続される。

【 0 0 1 8 】

上記ライセンス発行装置によれば、利用者は、ライセンス発行装置と距離的に離れた所においても、ネットワークを介してライセンス発行装置にアクセス可能な携帯端末などを用いて、ライセンス情報の発行を受けることができる。

【 0 0 1 9 】

この発明のもう 1 つの局面に従うと、コンテンツ再生装置は、暗号化されたコンテンツを復号して再生するものである。また、コンテンツ再生装置は、携帯可能なライセンス記憶装置の装置 ID を用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものである。ライセンス記憶装置は、自己を一意に識別することができる装置 ID と相手装置の正当性を認証する機能とを有する。そして、コンテンツ再生装置は、認証手段と、復号手段と、再生手段とを備える。認証手段は、利用者が携帯するライセンス記憶装置の正当性を認証する。復号手段は、利用者が携帯するライセンス記憶装置が正当なものであると認証手段によって認証されたとき、利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、当該ライセンス記憶装置の装置 ID を用いて復号する。再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【 0 0 2 0 】

上記コンテンツ再生装置では、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報を用いて暗号化コンテンツを復号し再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、ライセンス記憶装置に対応したさまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【 0 0 2 1 】

また、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報は、当該ライセンス記憶装置の装置 ID を用いて復号される。これにより、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【 0 0 2 2 】

好ましくは、上記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを復号するための復号化鍵を含む。そして、上記再生手段は、復号手段によって得られたライセンス情報に含まれる復号化鍵を用いて、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号する。

【 0 0 2 3 】

好ましくは、上記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを識別するためのコンテンツIDを含む。そして、上記再生手段は、復号手段によって得られたライセンス情報に含まれるコンテンツIDを用いて、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを取得する。

【 0 0 2 4 】

好ましくは、上記コンテンツ再生装置はさらに、蓄積手段を備える。蓄積手段は、暗号化されたコンテンツを蓄積する。そして、上記再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを蓄積手段から取得する。

【 0 0 2 5 】

上記コンテンツ再生装置では、再生する可能性のあるコンテンツをあらかじめすべて蓄積手段に蓄積しておくことにより、取得するのに時間のかかる大容量のコンテンツであっても即座に再生することができる。

【 0 0 2 6 】

好ましくは、上記再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得する。

【 0 0 2 7 】

上記コンテンツ再生装置では、コンテンツの再生時にその都度暗号化コンテンツをネットワークを介して取得する。これにより、仮想的に容量が無限大のコンテンツサーバを所有することと同様の効果が得られる。

【 0 0 2 8 】

好ましくは、上記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含む。そして、上記再生手段は、復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件に従って、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【 0 0 2 9 】

好ましくは、上記コンテンツ再生装置はさらに、コンテンツ利用条件更新手段と、更新後ライセンス情報生成手段と、暗号化手段と、書き換え手段とを備える。コンテンツ利用条件更新手段は、復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件を、再生手段によるコンテンツの再生に応じて更新する。更新後ライセンス情報生成手段は、復号手段によって得られたライセンス情報に含まれるコンテンツ利用条件に代えてコンテンツ利用条件更新手段によって更新されたコンテンツ利用条件を含んだ更新後ライセンス情報を生成する。暗号化手段は、更新後ライセンス情報生成手段によって生成された更新後ライセンス情報を利用者が携帯するライセンス記憶装置の装置IDを用いて暗号化する。書き換え手段は、利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、暗号化手段によって暗号化された更新後ライセンス情報に書き換える。

【 0 0 3 0 】

上記コンテンツ再生装置では、コンテンツの再生に応じてコンテンツ利用条件が変化する場合でも、コンテンツ利用条件を更新することができ、正しいコンテンツ利用条件を保持することができる。

【 0 0 . 3 1 】

この発明のさらにもう1つの局面に従うと、コンテンツ再生装置は、暗号化されたコンテンツを復号して再生するものである。また、コンテンツ再生装置は、携帯可能なライセンス記憶装置の装置鍵を用いて暗号化された当該ライセンス記憶装置の装置ID、を用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものである。ライセン

ス記憶装置は、自己を一意に識別することができる装置 I D と相手装置の正当性を認証する機能とを有する。そして、コンテンツ再生装置は、認証手段と、復号手段と、再生手段とを備える。認証手段は、利用者が携帯するライセンス記憶装置の正当性を認証し、当該ライセンス記憶装置が正当であると認証されたとき、当該ライセンス記憶装置の装置鍵を用いて当該ライセンス記憶装置の装置 I D を暗号化して暗号化装置 I D を生成する。復号手段は、利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、認証手段によって生成された暗号化装置 I D を用いて復号する。再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【 0 0 3 2 】

この発明のさらにもう 1 つの局面に従うと、ライセンス発行方法は、携帯可能なライセンス記憶装置に、コンテンツの利用を許可するライセンス情報を書き込むものである。ライセンス記憶装置は、自己を一意に識別することができる装置 I D と相手装置の正当性を認証する機能とを有する。そして、ライセンス発行方法は、認証ステップと、書き込みステップとを備える。認証ステップでは、利用者が携帯するライセンス記憶装置の正当性を認証する。書き込みステップでは、利用者が携帯するライセンス記憶装置が正当なものであると認証ステップによって認証されたとき、利用者によって指定されたコンテンツの利用を許可するライセンス情報を利用者が携帯するライセンス記憶装置の装置 I D を用いて暗号化して、当該暗号化したライセンス情報を利用者が携帯するライセンス記憶装置に書き込む。

【 0 0 3 3 】

上記ライセンス発行方法では、利用者が希望するコンテンツのライセンス情報を、携帯可能な独立したハードウェアであるライセンス記憶装置に書き込む。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、さまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【 0 0 3 4 】

また、ライセンス情報は、ライセンス記憶装置の装置IDを用いて暗号化される。これにより、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0035】

また、上記ライセンス発行方法では、コンテンツのライセンス情報だけを利用者の携帯するライセンス記憶装置に書き込む。したがって、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、利用者はライセンス記憶装置の記憶容量を気にする必要もない。

【0036】

また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は1つのライセンス記憶装置でたくさんのコンテンツを利用することができる。

【0037】

この発明のさらにもう1つの局面に従うと、コンテンツ再生方法は、暗号化されたコンテンツを復号して再生するものである。また、コンテンツ再生方法は、携帯可能なライセンス記憶装置の装置IDを用いて暗号化されて当該ライセンス記憶装置に記憶されたライセンス情報に基づいてコンテンツを復号して再生するものである。ライセンス記憶装置は、自己を一意に識別することができる装置IDと相手装置の正当性を認証する機能とを有する。そして、コンテンツ再生方法は、認証ステップと、復号ステップと、再生ステップとを備える。認証ステップでは、利用者が携帯するライセンス記憶装置の正当性を認証する。復号ステップでは、認証ステップにおいて利用者が携帯するライセンス記憶装置が正当なものであると認証されたとき、当該利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、当該ライセンス記憶装置の装置IDを用いて復号する。再生ステップでは、復号ステップによって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【0038】

上記コンテンツ再生方法では、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報を用いて暗号化コンテンツを復号し再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、さまざまな形態のコンテンツの提供を受けることができる。

【0039】

また、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報は、当該ライセンス記憶装置の装置IDを用いて復号される。これにより、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0040】

好ましくは、上記再生ステップでは、復号ステップによって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得する。

【0041】

上記コンテンツ再生方法では、コンテンツの再生時にその都度暗号化コンテンツをネットワークを介して取得する。これにより、仮想的に容量が無限大のコンテンツサーバを所有することと同様の効果が得られる。

【0042】

好ましくは、上記利用者が携帯するライセンス記憶装置に記憶されたライセンス情報は、当該ライセンス情報において利用を許可されているコンテンツを利用する際の制限事項を示すコンテンツ利用条件を含むものである。そして、上記再生ステップでは、復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件に従って、当該ライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツを復号して再生する。

【0043】

好ましくは、上記コンテンツ再生方法はさらに、更新ステップと、暗号化ステップと、書き換えステップとを備える。更新ステップでは、復号ステップによって得られたライセンス情報に含まれるコンテンツ利用条件を、再生ステップにおけるコンテンツの再生に応じて更新する。暗号化ステップでは、復号ステップに

よって得られたライセンス情報に含まれるコンテンツ利用条件に代えて更新ステップによって更新されたコンテンツ利用条件を含んだ更新後ライセンス情報を、利用者が携帯するライセンス記憶装置の装置IDを用いて暗号化する。書き換えステップでは、利用者が携帯するライセンス記憶装置に記憶されたライセンス情報を、暗号化ステップによって暗号化された更新後ライセンス情報に書き換える。

【 0 0 4 4 】

上記コンテンツ再生方法では、コンテンツの再生に応じてコンテンツ利用条件が変化する場合でも、コンテンツ利用条件を更新することができ、正しいコンテンツ利用条件を保持することができる。

【 0 0 4 5 】

【発明の実施の形態】

以下、この発明の実施の形態を図面を参照して詳しく説明する。なお、図中同一または相当部分には同一符号を付し、その説明は繰り返さない。また、この発明では暗号アルゴリズムに制限を設けていないが、以下の実施の形態における説明では、特に断りのない限り暗号アルゴリズムとして暗号鍵と復号鍵に同一の鍵を用いる共通鍵暗号方式を想定している。

【 0 0 4 6 】

(第1の実施形態)

図1は、この発明の第1の実施形態によるコンテンツ提供システムの構成を示す図である。図1を参照して、このコンテンツ提供システムでは、ソフトウェア、音楽、映像などの電子的な著作物であるデジタルコンテンツ（以下、コンテンツという。）と、当該コンテンツの利用を許可するライセンス情報とが分離して配布される。コンテンツは、そのままでは利用ができないように暗号化して暗号化コンテンツとして配布される。また、暗号化コンテンツは、ネットワーク、放送、パッケージなどさまざまな形態で配布される。

【 0 0 4 7 】

コンテンツの提供を希望する利用者は、メモリカード100をライセンス発行装置200に挿入する。ライセンス発行装置200は、利用者が希望するコンテ

コンテンツの利用を許可するライセンス情報を、利用者が携帯するメモリカード 1 0 0 の装置 ID を用いて暗号化して、当該メモリカード 1 0 0 に書き込む。すなわち、メモリカード 1 0 0 には暗号化ライセンス情報だけが書き込まれる。そして利用者は、暗号化ライセンス情報が書き込まれたメモリカード 1 0 0 をコンテンツ再生装置 3 0 0 に挿入する。コンテンツ再生装置 3 0 0 は、利用者が携帯するメモリカード 1 0 0 に書き込まれたライセンス情報を、当該メモリカード 1 0 0 の装置 ID を用いて復号する。そして、コンテンツ再生装置 3 0 0 は、復号したライセンス情報において利用を許可されているコンテンツに対応する暗号化コンテンツを復号して再生する。このようにして、コンテンツと、当該コンテンツの利用を許可するライセンス情報とが提供される。

【 0 0 4 8 】

以下、図 1 に示したメモリカード 1 0 0、ライセンス発行装置 2 0 0、およびコンテンツ再生装置 3 0 0 の具体的な構成、ライセンス発行装置 2 0 0 によるライセンス情報の発行の手順、ならびにコンテンツ再生装置 3 0 0 によるコンテンツの再生の手順について詳しく説明する。

【 0 0 4 9 】

図 2 は、図 1 に示したメモリカード 1 0 0 およびライセンス発行装置 2 0 0 の具体的な構成を示すブロック図である。以下、図 2 を参照しつつ説明する。

【 0 0 5 0 】

＜メモリカード 1 0 0 の構成＞

メモリカード 1 0 0 は、携帯可能な独立したハードウェアであり、自己を一意に識別可能な装置 ID を有する。そして、メモリカード 1 0 0 は、装置 ID 読み出し手段 1 1 0 と、相手装置認証手段 1 2 0 と、ライセンス記憶手段 1 3 0 とを備える。

【 0 0 5 1 】

装置 ID 読み出し手段 1 1 0 は、メモリカード 1 0 0 が有する装置 ID を読み出して出力する。

【 0 0 5 2 】

相手装置認証手段 1 2 0 は、ライセンス情報を送受信する相手装置が正当な装

置かどうかを認証する。相手装置は、ライセンス発行装置 2 0 0 からライセンス情報の提供を受ける場合にはライセンス発行装置 2 0 0 であり、コンテンツ再生装置 3 0 0 によってコンテンツの提供を受ける場合にはコンテンツ再生装置 3 0 0 である。相手装置認証手段 1 2 0 は、例えば、使用不可能なライセンス情報を発行してライセンス料のみを得るといような不正なライセンス発行装置を排除するために必要である。

【 0 0 5 3 】

ライセンス記憶手段 1 3 0 は、ライセンス発行装置 2 0 0 からの暗号化されたライセンス情報を記憶する。ライセンス記憶手段 1 3 0 としては、例えば、フラッシュメモリなどが挙げられる。

【 0 0 5 4 】

＜ライセンス発行装置 2 0 0 の構成＞

ライセンス発行装置 2 0 0 は、メモリカード認証手段 2 1 0 と、コンテンツ ID 入力手段 2 2 0 と、コンテンツ利用条件入力手段 2 3 0 と、コンテンツ復号化鍵取得手段 2 4 0 と、連結手段 2 5 0 と、暗号化手段 2 6 0 とを備える。

【 0 0 5 5 】

メモリカード認証手段 2 1 0 は、メモリカード 1 0 0 が正当なものであるかどうかを認証する。メモリカード認証手段 2 1 0 は、認証に先立ってメモリカード 1 0 0 から装置 ID を取得する。そしてメモリカード 1 0 0 との間で相互に認証を行った後、装置 ID を暗号化して暗号化装置 ID を出力する。これは、コンテンツを再生する際にコンテンツ再生装置 3 0 0 で同一の鍵を得るためである。

【 0 0 5 6 】

コンテンツ ID 入力手段 2 2 0 は、利用者が指定したコンテンツに対するコンテンツ ID を出力する。コンテンツ ID とは、各コンテンツを識別するための記号である。コンテンツ ID 入力手段 2 2 0 としては、例えば、キーボードやタッチパネルなどの入力装置によって利用者に直接に所望のコンテンツに対応したコンテンツ ID の入力を促し、入力されたコンテンツ ID をそのまま出力するものが挙げられる。また、別の例としては、ライセンス情報の発行が可能なコンテンツタイトルの一覧をディスプレイなどに表示して利用者に選択を促し、選択され

だコンテンツタイトルに対するコンテンツIDを、図3に示すようなコンテンツタイトル31とコンテンツID32とが対応づけられたデータベースから取得するというものが挙げられる。なお、図3に示すデータベースでは、コンテンツタイトル31、コンテンツID32、およびコンテンツ復号化鍵33が対応づけられている。そして、コンテンツ復号化鍵33の情報は、外部から読み出すことができないように保護されている。

【0057】

コンテンツ利用条件入力手段230は、コンテンツ利用条件を出力する。コンテンツ利用条件とは、コンテンツを利用する際の制限事項を示す情報である。コンテンツ利用条件としては、例えば、コンテンツがソフトウェアプログラムである場合に、「扱うデータ量は100Kバイトまでとする」というような制限事項を示す情報が挙げられる。また、別の例としては、コンテンツが音楽データの場合に、「再生することができる期間」を示す情報が挙げられる。コンテンツ利用条件はコンテンツの特性に応じてさまざまなものが考えられるため、コンテンツまたはコンテンツのカテゴリに対応した利用条件データベースを設けてもよい。この場合にも、上述したコンテンツID入力手段220におけるのと同様に、利用者に利用条件の一覧を提示して利用者に選択を促すなどの方法がある。

【0058】

コンテンツ復号化鍵取得手段240は、コンテンツID入力手段220からのコンテンツIDを受け、当該コンテンツIDに対応するコンテンツを暗号化された状態から復号するための鍵を取得する。例えば、図3に示したデータベースを参照して取得することができる。

【0059】

連結手段250は、コンテンツID入力手段220からのコンテンツID、コンテンツ利用条件入力手段230からのコンテンツ利用条件、およびコンテンツ復号化鍵取得手段240からのコンテンツ復号化鍵を連結してライセンス情報を生成する。

【0060】

暗号化手段260は、連結手段250によって生成されたライセンス情報をメ

メモリカード認証手段 2 1 0 からの暗号化装置 I D で暗号化して暗号化ライセンス情報を生成する。そして、暗号化手段 2 6 0 は、暗号化ライセンス情報をメモリカード 1 0 0 のライセンス記憶手段 1 3 0 へ書き込む。

【 0 0 6 1 】

< ライセンス情報の発行の手順 >

図 4 は、図 2 に示したライセンス発行装置 2 0 0 によるライセンス情報の発行の手順を示すフローチャートである。以下、図 4 および図 2 を参照しつつライセンス情報の発行の手順について説明する。

【 0 0 6 2 】

まず、ステップ S T 4 0 1 において、利用者は、メモリカード 1 0 0 をライセンス発行装置 2 0 0 の所定の挿入口に差し込む。これにより、メモリカード 1 0 0 に設けられたピンとライセンス発行装置 2 0 0 のソケットとの間が電氣的に接続される。この結果、メモリカード 1 0 0 とライセンス発行装置 2 0 0 との間で、お互いにデータを送受信するための通信手段が確保される。

【 0 0 6 3 】

次いで、ステップ S T 4 0 2 において、メモリカード 1 0 0 とライセンス発行装置 2 0 0 との間で、お互いが正当な装置であることの認証が行われる。この相互認証の手順については後述する。相互認証中にエラーが発生した場合には処理が中断されて利用者にその旨が知らされる。相互認証を行った後、メモリカード認証手段 2 1 0 は、メモリカード 1 0 0 の装置 I D を暗号化して暗号化装置 I D を生成する。

【 0 0 6 4 】

次いで、ステップ S T 4 0 3 において、利用者は、コンテンツ I D 入力手段 2 2 0 を利用して、希望するコンテンツに対応するコンテンツ I D を入力する。これにより、利用者が希望するコンテンツに対応するコンテンツ I D が得られる。

【 0 0 6 5 】

次いで、ステップ S T 4 0 4 において、利用者は、コンテンツ利用条件入力手段 2 3 0 を利用して、コンテンツ利用条件を入力する。これにより、利用者が希望するコンテンツに対するコンテンツ利用条件が得られる。

【 0 0 6 6 】

次いで、ステップ S T 4 0 5 において、利用者は、希望するコンテンツおよびその利用条件に対応した料金を支払う。料金の支払い手段／方法としては、種々の公知の手段／方法を利用することができる。

【 0 0 6 7 】

次いで、ステップ S T 4 0 6 において、コンテンツ復号化鍵取得手段 2 4 0 は、ステップ S T 4 0 3 において得られたコンテンツ I D に対応するコンテンツを暗号化された状態から復号するための鍵を取得する。ここでは、図 3 に示したデータベースを参照して取得する。

【 0 0 6 8 】

次いで、ステップ S T 4 0 7 において、連結手段 2 5 0 は、ステップ S T 4 0 3 において得られたコンテンツ I D、ステップ S T 4 0 4 において得られたコンテンツ利用条件、およびステップ S T 4 0 6 において得られたコンテンツ復号化鍵を連結してライセンス情報を生成する。

【 0 0 6 9 】

次いで、ステップ S T 4 0 8 において、暗号化手段 2 6 0 は、ステップ S T 4 0 7 において得られたライセンス情報をステップ S T 4 0 2 において得られた暗号化装置 I D で暗号化して暗号化ライセンス情報を生成する。

【 0 0 7 0 】

次いで、ステップ S T 4 0 9 において、暗号化手段 2 6 0 は、ステップ S T 4 0 8 において得られた暗号化ライセンス情報をメモリカード 1 0 0 のライセンス記憶手段 1 3 0 へ書き込む。通常、メモリカード 1 0 0 のライセンス記憶手段 1 3 0 には、複数のコンテンツの暗号化ライセンス情報が記憶される。そこで、ライセンス記憶手段 1 3 0 に暗号化ライセンス情報を書き込む際には、図 5 に示すように、暗号化ライセンス情報 5 3 に対応づけてコンテンツタイトル 5 1、コンテンツ付属情報 5 2 など書き込んでおく。これにより、後で利用者が、複数の暗号化ライセンス情報から希望のコンテンツを指示することが容易となる。

【 0 0 7 1 】

このようにして、利用者の希望するコンテンツのライセンス情報が、利用者の

携帯するメモリカード 1 0 0 のライセンス記憶手段 1 3 0 に書き込まれる。

【 0 0 7 2 】

以上のように、第 1 の実施形態におけるライセンス発行装置 2 0 0 は、メモリカード認証手段 2 1 0 と、暗号化手段 2 6 0 とを設けたため、コンテンツと分離したライセンス情報を、正当と認識されたメモリカード 1 0 0 へ記憶させることができる。

【 0 0 7 3 】

また、利用者が希望するコンテンツ自体は書き込まずにそのコンテンツのライセンス情報だけを、利用者の携帯するメモリカード 1 0 0 に書き込む。したがって、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、メモリカード 1 0 0 のライセンス記憶手段 1 3 0 の記憶容量を気にする必要もない。

【 0 0 7 4 】

また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は 1 つのメモリカード 1 0 0 でたくさんのコンテンツを利用することができる。

【 0 0 7 5 】

なお、ここでは、連結手段 2 5 0 によって生成されるライセンス情報にはコンテンツ利用条件が含まれているが、コンテンツ利用条件を用いずにコンテンツ ID とコンテンツ復号化鍵とを連結してライセンス情報を生成してもよい。この場合は、コンテンツ利用条件入力手段 2 3 0 を設ける必要はない。

【 0 0 7 6 】

また、コンテンツ復号化鍵を用いずにコンテンツ ID とコンテンツ利用条件とを連結してライセンス情報を生成してもよい。この場合、ライセンス発行装置 2 0 0 にコンテンツ復号化鍵取得手段 2 4 0 を設ける必要はなくなるが、その代わりに、コンテンツ再生装置 3 0 0 にコンテンツ復号化鍵取得手段を設ける必要がある。

【 0 0 7 7 】

< 相互認証の手順 >

次に、図4に示したステップST402における相互認証の手順について、図6および図2を参照しつつ説明する。なお、図6中、ステップST601-ST606はメモリカード100の相手装置認証手段120における処理、ステップST611-ST616はライセンス発行装置200のメモリカード認証手段210における処理を示す。

【0078】

認証に先立って、ライセンス発行装置200のメモリカード認証手段210は、メモリカード100から装置ID(id)を取得する。このように、メモリカード100およびライセンス発行装置200は、あらかじめメモリカード100の装置ID(id)を共有しておく。さらに、メモリカード100は装置鍵Kd1を、ライセンス発行装置200は装置鍵Kd2を持つ。装置鍵Kd1, Kd2は、それぞれの装置自身で保持し、外部から読み出しできないようにしておく。望ましくは、解析できないような耐タンパー装置で防御されている。メモリカード100およびライセンス発行装置200がお互いに正当な装置であれば、装置鍵Kd1と装置鍵Kd2は同一であるものとする。

【0079】

まず、ステップST601において、メモリカード100の相手装置認証手段120は、暗号化装置ID(Ei1)を生成する。暗号化装置ID(Ei1)は、メモリカード100の装置ID(id)を装置鍵Kd1を用いて暗号化することによって生成される。これを図6では、 $Ei1 = F(Kd1, id)$ と表している。

【0080】

一方、ステップST611において、ライセンス発行装置200のメモリカード認証手段210は、暗号化装置ID(Ei2)を生成する。暗号化装置ID(Ei2)は、メモリカード100の装置ID(id)を装置鍵Kd2を用いて暗号化することによって生成される。これを図6では、 $Ei2 = F(Kd2, id)$ と表している。

【0081】

そして以下の処理によって、お互いが有する暗号化装置ID(Ei1, Ei2

）が同一であることを、暗号化装置ID (E_{i1} , E_{i2}) を装置外部の通信手段を用いてやりとりすることなく確認することによって、お互いの装置の正当性を認証する。

【0082】

ステップST602において、メモリカード100の相手装置認証手段120は、乱数 R_1 を生成し、ライセンス発行装置200のメモリカード認証手段210へ送信する。

【0083】

そして、ステップST603において、メモリカード100の相手装置認証手段120は、乱数 R_1 を暗号化装置ID (E_{i1}) を用いて暗号化して暗号化乱数 E_{1r1} を生成する。これを図6では、 $E_{1r1} = E(E_{i1}, R_1)$ と表している。

【0084】

一方、ステップST612において、ライセンス発行装置200のメモリカード認証手段210は、受信した乱数 R_1 を暗号化装置ID (E_{i2}) を用いて暗号化して暗号化乱数 E_{2r1} を生成する。これを図6では、 $E_{2r1} = E(E_{i2}, R_1)$ と表している。そして、ライセンス発行装置200のメモリカード認証手段210は、暗号化乱数 E_{2r1} をメモリカード100の相手装置認証手段120へ送信する。

【0085】

次いで、ステップST604において、メモリカード100の相手装置認証手段120は、ステップST603において生成した暗号化乱数 E_{1r1} と、ステップST612において受信した暗号化乱数 E_{2r1} とを比較する。比較の結果、両者が一致しないときは、ステップST606に進み、相手装置認証手段120は、ライセンス発行装置200が正当なものではないとみなし（エラー発生）、利用者にその旨を知らせる。そして処理を終了する。一方、両者が一致するときは、相手装置認証手段120は、ライセンス発行装置200が正当なものであるとみなし、ステップST605に進む。

【0086】

ステップ S T 6 1 3 において、ライセンス発行装置 2 0 0 のメモリカード認証手段 2 1 0 は、乱数 R 2 を生成し、メモリカード 1 0 0 の相手装置認証手段 1 2 0 へ送信する。

【 0 0 8 7 】

そして、ステップ S T 6 1 4 において、ライセンス発行装置 2 0 0 のメモリカード認証手段 2 1 0 は、乱数 R 2 を暗号化装置 I D (E i 2) を用いて暗号化して暗号化乱数 E 2 r 2 を生成する。これを図 6 では、 $E 2 r 2 = E (E i 2 , R 2)$ と表している。

【 0 0 8 8 】

一方、ステップ S T 6 0 5 において、メモリカード 1 0 0 の相手装置認証手段 1 2 0 は、受信した乱数 R 2 を暗号化装置 I D (E i 1) を用いて暗号化して暗号化乱数 E 1 r 2 を生成する。これを図 6 では、 $E 1 r 2 = E (E i 1 , R 2)$ と表している。そして、メモリカード 1 0 0 の相手装置認証手段 1 2 0 は、暗号化乱数 E 1 r 2 をライセンス発行装置 2 0 0 のメモリカード認証手段 2 1 0 へ送信する。

【 0 0 8 9 】

次いで、ステップ S T 6 1 5 において、ライセンス発行装置 2 0 0 のメモリカード認証手段 2 1 0 は、ステップ S T 6 1 4 において生成した暗号化乱数 E 2 r 2 と、ステップ S T 6 0 5 において受信した暗号化乱数 E 1 r 2 とを比較する。比較の結果、両者が一致しないときは、ステップ S T 6 1 6 に進み、ライセンス発行装置 2 0 0 のメモリカード認証手段 2 1 0 は、メモリカード 1 0 0 が正当なものではないとみなし（エラー発生）、利用者にその旨を知らせる。そして処理を終了する。一方、両者が一致するときは、ライセンス発行装置 2 0 0 のメモリカード認証手段 2 1 0 は、メモリカード 1 0 0 が正当なものであるとみなす。

【 0 0 9 0 】

以上のようにして、メモリカード 1 0 0 とライセンス発行装置 2 0 0 との間で、お互いが正当な装置であることの認証（相互認証）が行われる。

【 0 0 9 1 】

そして、相互認証の手続きが終了した後、メモリカード認証手段 2 1 0 は、暗

号化装置ID (Ei2) を暗号化手段260へ出力する。

【0092】

なお、ここでは装置鍵Kd1, Kd2を用いているが、これらを用いず、装置IDに特定の変換Fを施してEi1, Ei2を得ることもできる。この場合は、変換Fを非公開にして、変換方法が共通である装置を正当な装置を認証することとなる。

【0093】

＜コンテンツ再生装置300の構成＞

図7は、図1に示したメモリカード100およびコンテンツ再生装置300の具体的な構成を示すブロック図である。以下、図7を参照してコンテンツ再生装置300の具体的な構成について説明する。

【0094】

コンテンツ再生装置300は、メモリカード認証手段210と、コンテンツID入力手段220と、復号手段310と、分離手段320と、比較手段330と、再生手段340と、暗号化コンテンツデータベース350とを備える。

【0095】

復号手段310は、メモリカード100のライセンス記憶手段130に記憶された暗号化ライセンス情報を読み出し、読み出した暗号化ライセンス情報をメモリカード認証手段210からの暗号化装置IDを用いて復号してライセンス情報を得る。

【0096】

分離手段320は、復号手段310によって得られたライセンス情報から、コンテンツID、コンテンツ利用条件、およびコンテンツ復号化鍵を得る。

【0097】

比較手段330は、分離手段によって得られたコンテンツIDとコンテンツID入力手段220によって得られたコンテンツIDとを比較し、両者が一致するときは、再生指示信号を再生手段340に出力する。

【0098】

暗号化コンテンツデータベース350には、コンテンツをそのままでは利用が

できないように暗号化した暗号化コンテンツが格納されている。

【 0 0 9 9 】

再生手段 3 4 0 は、比較手段 3 3 0 からの再生指示信号に応答して、分離手段 3 2 0 によって得られたコンテンツ ID に対応する暗号化コンテンツを暗号化コンテンツデータベース 3 5 0 から取得する。そして再生手段 3 4 0 は、取得した暗号化コンテンツを分離手段 3 2 0 によって得られたコンテンツ復号化鍵を用いて復号し、分離手段 3 2 0 によって得られたコンテンツ利用条件に従って再生する。

【 0 1 0 0 】

<コンテンツの再生の手順>

図 8 は、図 7 に示したコンテンツ再生装置 3 0 0 によるコンテンツの再生の手順を示すフローチャートである。以下、図 8 および図 7 を参照しつつコンテンツの再生の手順について説明する。

【 0 1 0 1 】

まず、ステップ S T 8 0 1 において、利用者は、再生を希望するコンテンツに対する暗号化ライセンス情報が記憶されたメモリカード 1 0 0 をコンテンツ再生装置 3 0 0 の所定の挿入口に差し込む。これにより、メモリカード 1 0 0 に設けられたピンとコンテンツ再生装置 3 0 0 のソケットとの間が電氣的に接続される。この結果、メモリカード 1 0 0 とコンテンツ再生装置 3 0 0 との間で、お互いにデータを送受信するための通信手段が確保される。

【 0 1 0 2 】

次いで、ステップ S T 8 0 2 において、メモリカード 1 0 0 とコンテンツ再生装置 3 0 0 との間で、お互いが正当な装置であることの認証が行われる。この相互認証は、図 6 に示したのと同様の手順で行われる。相互認証を行った後、コンテンツ再生装置 3 0 0 のメモリカード認証手段 2 1 0 は、メモリカード 1 0 0 の装置 ID を暗号化して暗号化装置 ID を生成する。

【 0 1 0 3 】

次いで、ステップ S T 8 0 3 において、利用者は、コンテンツ ID 入力手段 2 2 0 を利用して、再生を希望するコンテンツに対するコンテンツ ID を入力する

。通常、メモリカード100のライセンス記憶手段130には、複数の暗号化ライセンス情報が記憶されている。しかし、図5に示したように、メモリカード100のライセンス記憶手段130には、暗号化ライセンス情報53に対応づけてコンテンツタイトル51、コンテンツ付属情報52なども記憶されている。したがって、メモリカード100のライセンス記憶手段130に記憶されているコンテンツタイトル／コンテンツ付属情報の一覧を利用者に提示して、希望するコンテンツタイトルを選択させた後、図3に示したのと同様のデータベースを用いてコンテンツIDを得ることができる。

【0104】

次いで、ステップST804において、復号手段310は、メモリカード100のライセンス記憶手段130から、利用者が再生を希望するコンテンツに対する暗号化ライセンス情報を読み出す。ここでは、ステップST803において利用者が選択したコンテンツタイトルを用いることによって、復号すべき暗号化ライセンス情報を容易に特定することができる。そして、復号手段310は、読み出した暗号化ライセンス情報を、ステップST802においてメモリカード認証手段210によって生成された暗号化装置IDを用いて復号し、ライセンス情報を得る。

【0105】

次いで、ステップST805において、分離手段330は、復号手段310によって得られたライセンス情報を、コンテンツID、コンテンツ復号化鍵、およびコンテンツ利用条件に分離する。

【0106】

次いで、ステップST806において、比較手段330は、ステップST803においてコンテンツID入力手段220によって得られたコンテンツIDと、ステップST805において分離手段320によって得られたコンテンツIDとを比較する。比較の結果、両者が同一であれば、このライセンス情報は正当なライセンス発行装置によって発行されたものであるとみなし、比較手段330は、再生指示信号を再生手段340に出力する。

【0107】

次いで、ステップ S T 8 0 7 において、再生手段 3 4 0 は、比較手段 3 3 0 からの再生指示信号に応答して、分離手段 3 2 0 によって得られたコンテンツ I D に対応する暗号化コンテンツを暗号化コンテンツデータベース 3 5 0 から取得する。そして再生手段 3 4 0 は、取得した暗号化コンテンツを分離手段 3 2 0 によって得られたコンテンツ復号化鍵を用いて復号し、分離手段 3 2 0 によって得られたコンテンツ利用条件に従って再生する。例えば、コンテンツ利用条件として利用可能な期限が付加されたものであれば、現在の日付と利用可能な期限とを比較することにより、再生を行うかどうかを再生前に判断する。

【 0 1 0 8 】

このようにして、利用者が希望するコンテンツの再生が行われる。

【 0 1 0 9 】

以上のように、第 1 の実施形態におけるコンテンツ再生装置 3 0 0 は、メモリカード認証手段 2 1 0 と、復号手段 3 1 0 と、再生手段 3 4 0 とを設けたため、コンテンツと分離したライセンス情報を、正当と認識されたメモリカード 1 0 0 から読み込んで、対応するコンテンツを再生することができる。

【 0 1 1 0 】

なお、ここでは、暗号化コンテンツデータベース 3 5 0 をコンテンツ再生装置 3 0 0 内に設けたが、これを外部、例えば、通信回線を介して遠隔地に設けてもよい。この場合、コンテンツ再生装置 3 0 0 は、コンテンツ I D のような情報でコンテンツを特定して、外部にある暗号化コンテンツデータベースより暗号化コンテンツを受信し、再生する。このように暗号化コンテンツデータベースを外部に設けることは、コンテンツ再生装置が大きな記憶容量を確保できない携帯端末である場合に有利である。

【 0 1 1 1 】

また、メモリカード 1 0 0 のライセンス記憶手段 1 3 0 に記憶されたライセンス情報にコンテンツ利用条件が含まれていない場合には、分離手段 3 2 0 ではコンテンツ利用条件は得られない。したがって、コンテンツ再生手段 3 4 0 は利用条件を考慮する必要はない。

【 0 1 1 2 】

また、メモリカード100のライセンス記憶手段130に記憶されたライセンス情報にコンテンツ復号化鍵が含まれていない場合には、図5に示したようなコンテンツIDとコンテンツ復号化鍵とを対応づけたデータベースを設けておき、このデータベースを用いて、分離手段320によって得られたコンテンツIDよりコンテンツ復号化鍵を得ることができる。

【0113】

また、メモリカード100のライセンス記憶手段130から読み込んだ暗号化ライセンス情報が十分信頼できるものである場合には、コンテンツID入力手段220および比較手段330を取り除いた構成とすることも可能である。

【0114】

また、図2に示したライセンス発行装置200の暗号化手段260および図7に示したコンテンツ再生装置300の復号化手段310では、暗号／復号の鍵としてメモリカード認証手段210からの暗号化装置IDを用いているが、これに代えて、外部から読み出し不可能な非公開の鍵をライセンス発行装置200およびコンテンツ再生装置300にあらかじめ記憶させておき、これを暗号／復号の鍵としてもよい。さらにこの場合、暗号化／復号化の暗号アルゴリズムとして、例えばRSAのような非対称暗号を用い、それぞれの装置で対応する鍵を記憶しておくこともできる。

【0115】

<効果>

以上のように、この発明の第1の実施形態によるコンテンツ提供システムでは、ライセンス発行装置200は、コンテンツのライセンス情報を、携帯可能な独立したハードウェアであるメモリカード100に書き込む。そして、コンテンツ再生装置300は、メモリカード100に記憶されたライセンス情報に従ってコンテンツを再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたメモリカード100を携帯し、ライセンス発行装置200に対応したさまざまな形態のコンテンツ再生装置300を利用してコンテンツの提供を受けることができる。すなわち、利用者は、コンテンツ再生装置300の形態に制限されることなく、購入したコンテンツを利用することができる。

【 0 1 1 6 】

また、ライセンス情報は、暗号化装置 I D を用いて暗号化／復号化される。すなわち、ライセンス情報は、個々のメモリカード 1 0 0 を一意に識別可能な装置 I D を用いて暗号化／復号化される。これにより、暗号化ライセンス情報を不正にコピーしたメモリカードを用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【 0 1 1 7 】

また、ライセンス発行装置 2 0 0 はコンテンツのライセンス情報だけを、利用者の携帯するメモリカード 1 0 0 に書き込む。したがって、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、メモリカード 1 0 0 のライセンス記憶手段 1 3 0 の記憶容量を気にする必要もない。

【 0 1 1 8 】

また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は 1 つのメモリカード 1 0 0 でたくさんのコンテンツを利用することができる。

【 0 1 1 9 】

また、コンテンツは暗号化されて配布され、ライセンス情報を購入しなければ再生が不可能なため、ネットワーク、放送、パッケージなど形態を問わず自由に流通させることが可能となり、かつ、利用者にとっては入手が容易となる。これにより、利用者は必ずしもコンテンツを所有する必要がなく、ライセンス情報のみを購入、携帯し、必要に応じてコンテンツにアクセスすればよい。この結果、利用者側でコンテンツを蓄積するための大容量のデータ蓄積装置を確保できない場合は、コンテンツの再生時にその都度ダウンロードすることによって、仮想的に容量が無限大のコンテンツサーバを所有することと同様の効果が得られる。一方、利用者側に大容量のデータ蓄積装置を確保できる場合は、事前に再生する可能性のあるコンテンツをすべてダウンロードしておき、再生時にはライセンス情報を購入することによって、ダウンロードに時間のかかる大容量のコンテンツを即座に再生することが可能となる。

【 0 1 2 0 】

(第 2 の実施形態)

この発明の第 2 の実施形態によるコンテンツ提供システムでは、図 7 に示したコンテンツ再生システム 3 0 0 に代えて、図 9 に示すコンテンツ再生装置 9 0 0 を備える。そして、その他の構成を第 1 の実施形態におけるコンテンツ提供システムと同じくする。

【 0 1 2 1 】

<コンテンツ再生装置 9 0 0 の構成>

図 9 を参照して、このコンテンツ再生装置 9 0 0 は、メモリカード認証手段 2 1 0 と、コンテンツ ID 入力手段 2 2 0 と、復号手段 3 1 0 と、分離手段 3 2 0 と、比較手段 3 3 0 と、再生手段 3 4 0 と、暗号化コンテンツデータベース 3 5 0 と、コンテンツ利用条件更新手段 9 1 0 と、連結手段 9 2 0 と、暗号化手段 9 3 0 と、暗号化ライセンス情報更新手段 9 4 0 とを備える。

【 0 1 2 2 】

再生手段 3 4 0 は、第 1 の実施形態において説明した動作に加えてさらに、コンテンツを再生したことを示す再生検知信号を生成し、コンテンツ利用条件を出力する。

【 0 1 2 3 】

コンテンツ利用条件更新手段 9 1 0 は、コンテンツ再生手段 3 4 0 からの再生検知信号を受けて、コンテンツ再生手段 3 4 0 からコンテンツ利用条件を読み込み、当該コンテンツ利用条件を更新して更新後コンテンツ利用条件を生成する。これは、コンテンツの再生前後でコンテンツ利用条件が変化する場合（例えば、コンテンツ利用条件として「コンテンツを利用することができる回数」が定められている場合など）を想定している。このように利用回数に制限が存在する場合は、1 回再生するごとに残りの利用回数を減じていかなければならない。そして減じた後の利用回数を新たにコンテンツの利用条件として更新することが必要となる。

【 0 1 2 4 】

連結手段 9 2 0 は、コンテンツ利用条件更新手段 9 1 0 からの更新後コンテン

ツ利用条件と、分離手段 3 2 0 からのコンテンツ ID およびコンテンツ復号化鍵とを連結して、更新後ライセンス情報を生成する。

【 0 1 2 5 】

暗号化手段 9 3 0 は、連結手段 9 2 0 からの更新後ライセンス情報をメモリカード認証手段 2 1 0 からの暗号化装置 ID を用いて暗号化して、更新後暗号化ライセンス情報を生成する。

【 0 1 2 6 】

暗号化ライセンス情報更新手段 9 4 0 は、メモリカード 1 0 0 のライセンス記憶手段 1 3 0 に記憶されている暗号化ライセンス情報を、暗号化手段 9 3 0 によって生成された更新後暗号化ライセンス情報に書き換える。

【 0 1 2 7 】

<コンテンツ再生装置 9 0 0 の動作>

以下、図 9 に示したコンテンツ再生装置 9 0 0 の動作について説明する。

【 0 1 2 8 】

コンテンツ再生装置 9 0 0 は、図 8 に示したステップ ST 8 0 1 - ST 8 0 7 における処理と同様の処理によってコンテンツの再生を行う。

【 0 1 2 9 】

そして、コンテンツの再生が終了した後またはコンテンツの再生中に、再生手段 3 4 0 は、再生検知信号をコンテンツ利用条件更新手段 9 1 0 に出力する。

【 0 1 3 0 】

次いで、コンテンツ利用条件更新手段 9 1 0 は、再生検知信号を受けて、再生手段 3 4 0 からコンテンツ利用条件を読み込み、当該コンテンツ利用条件のうち再生に応じて変更すべき部分を変更する。例えば、コンテンツ利用条件が「再生可能な回数は 3 である」という条件であれば、再生可能な回数を 1 減じて 2 と変更する。そして、これを更新後コンテンツ利用条件として連結手段 9 2 0 へ出力する。

【 0 1 3 1 】

次いで、連結手段 9 2 0 は、更新後コンテンツ利用条件と、コンテンツ ID と、コンテンツ復号化鍵とを連結して、更新後ライセンス情報を生成する。

【 0 1 3 2 】

次いで、暗号化手段 9 3 0 は、更新後ライセンス情報を暗号化装置 I D を用いて暗号化する。

【 0 1 3 3 】

次いで、暗号化ライセンス情報更新手段 9 4 0 は、メモリカード 1 0 0 のライセンス記憶手段 1 3 0 に記憶されている暗号化ライセンス情報を消去し、更新後暗号化ライセンス情報を書き込む。

【 0 1 3 4 】

< 効果 >

以上のように、第 2 の実施形態によるコンテンツ再生装置 9 0 0 は、コンテンツ利用条件更新手段 9 1 0 と、連結手段 9 2 0 と、暗号化手段 9 3 0 と、暗号化ライセンス情報更新手段 9 4 0 とを設けたため、コンテンツの再生に応じてコンテンツ利用条件が変化する場合でも、コンテンツ利用条件を更新することができ、正しいコンテンツ利用条件を保持することが可能となる。

【 0 1 3 5 】

(第 3 の実施形態)

図 1 0 は、図 1 に示したコンテンツ提供システムの適用例を示す図である。以下、図 1 0 を参照して、コンテンツ提供システムの適用例について説明する。

【 0 1 3 6 】

ライセンス発行装置 2 0 0 は、駅、コンビニ、店頭などに設置されたり (2 0 0 a) 、パソコンや携帯電話などの端末 4 0 0 から有線、無線を問わずアクセス可能なネットワークに接続されたりする (2 0 0 b) 。そして、利用者は、ライセンス発行装置 2 0 0 a または端末 4 0 0 にメモリカード 1 0 0 を挿入し、ガイドンスに従って希望のコンテンツ (音楽、映画、ゲーム、電子本など) を選択して、表示された料金を支払う。ライセンス発行装置 2 0 0 a , 2 0 0 b は、利用者が選択したコンテンツに対するライセンス情報を、メモリカード 1 0 0 の装置 I D を用いて暗号化してメモリカード 1 0 0 へ書き込む。書き込みが終了すると、利用者はレシートを受け取り、メモリカード 1 0 0 を取り出す。このように、利用者は、自宅 / 外出先のいずれにおいても、希望するコンテンツの暗号化ライ

センス情報をメモリカード100に書き込むことができる。そして、利用者は、CDやMDなどの希望のコンテンツが格納された媒体を持ち歩く必要はなく、ライセンス情報だけが書き込まれたメモリカード100を携帯すればよい。

【0137】

一方、コンテンツは、そのままでは利用ができないように暗号化して暗号化コンテンツとして、ネットワーク、放送、パッケージなどのさまざまな形態で流通している。

【0138】

そして、利用者の自宅に設けられたホームサーバ350aには、パソコンからネットワーク経由でダウンロードした暗号化コンテンツや、デジタルTVのデータ放送を受信して得られた暗号化コンテンツなどが蓄積されている。利用者は、希望するコンテンツの暗号化ライセンス情報が書き込まれたメモリカードを自宅にあるコンテンツ再生装置300aに挿入することによって、コンテンツの提供を受けることができる。

【0139】

また、外出先（列車、飛行機などの交通機関、自動車、店、図書館、ホテルなど）にも、コンテンツサーバ350b、コンテンツ再生装置300bが設けられている。コンテンツ再生装置300bは、コンテンツの提供者側が用意するものであってもよいし、利用者が所持する携帯端末を利用してもよい。利用者は、希望するコンテンツの暗号化ライセンス情報が書き込まれたメモリカードをコンテンツ再生装置300bに挿入することによって、コンテンツの提供を受けることができる。

【0140】

コンテンツ提供者にとっては、豊富なコンテンツを提供することによる集客効果、差別化、徴収した利用料などのメリットが得られる。また、コンテンツの再生中にCMを流して広告収入を得たり、自店舗の紹介をしたりすることができる。さらに、高音質、高画質を売りにしたコンテンツ再生装置を用意して、その利用料を徴収することもできる（例えば、ハイビジョン映像なら100円増しにするなど）。

【0141】

利用者にとっては、好きな音楽を、自宅、車の中、電車の中、船の中、飛行機の中などで聴くことができる。しかも、CDやMDなどの媒体や再生装置を持ち歩く必要がなく、メモリカード1枚だけでよい。

【0142】

また、利用者は、最近はやりの個室スペースで、音楽を聴いたり、映画を見たり、本を読んだり、ゲームをしたりというようにさまざまなコンテンツを提供を受けることができる。この場合、個室スペースの提供者は、メモリカードにライセンス情報が書き込まれていれば個室スペースの利用料を無料とすることもできる。ライセンス発行装置が設けられていれば、利用者は、メモリカードにライセンス情報が書き込まれていない場合にも、その場で購入することができる。

【0143】

また、利用者は、旅行先で見所を調べるために、旅行前に買った雑誌（コンテンツ）へアクセスして調べることもできる。これにより、利用者は、雑誌、新聞、百科事典などを持ち歩く必要がなくなる。

【0144】

【発明の効果】

この発明の1つの局面に従ったライセンス発行装置は、利用者が希望するコンテンツのライセンス情報を、携帯可能な独立したハードウェアであるライセンス記憶装置に書き込む。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、ライセンス記憶装置に対応したさまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【0145】

また、ライセンス情報は、ライセンス記憶装置の装置IDを用いて暗号化されるため、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【0146】

また、コンテンツのライセンス情報だけを利用者の携帯するライセンス記憶装

置に書き込むため、利用者が希望するコンテンツが大容量のコンテンツであっても、ライセンス情報の発行にかかる時間を増大させることがなく、また、利用者はライセンス記憶装置の記憶容量を気にする必要もない。

【 0 1 4 7 】

また、ライセンス情報のデータ量はコンテンツのデータ量に比べて小さいため、利用者は1つのライセンス記憶装置でたくさんのコンテンツを利用することができる。

【 0 1 4 8 】

また、ライセンス発行装置は、利用者が携帯するライセンス記憶装置にネットワークを介して接続されるため、利用者はライセンス発行装置と距離的に離れた所にいても、ネットワークを介してライセンス発行装置にアクセス可能な携帯端末などを用いて、ライセンス情報の発行を受けることができる。

【 0 1 4 9 】

この発明のもう1つの局面に従ったコンテンツ再生装置は、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報を用いて暗号化コンテンツを復号し再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、ライセンス記憶装置に対応したさまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【 0 1 5 0 】

また、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報は、当該ライセンス記憶装置の装置IDを用いて復号されるため、暗号化ライセンス情報を不正にコピーしたライセンス記憶装置を用いてコンテンツの提供を受けるような不正な利用を防ぐことができる。

【 0 1 5 1 】

また、蓄積手段を設けたため、再生する可能性のあるコンテンツをあらかじめすべて蓄積しておくことができる。これにより、取得するのに時間のかかる大容量のコンテンツであっても即座に再生することができる。

【 0 1 5 2 】

また、再生手段は、復号手段によって得られたライセンス情報において利用を許可されているコンテンツに対応する暗号化されたコンテンツをネットワークを介して取得するため、コンテンツの再生時にその都度暗号化コンテンツをネットワークを介して取得することができる。これにより、仮想的に容量が無限大のコンテンツサーバを所有することと同様の効果が得られる。

【 0 1 5 3 】

また、コンテンツ利用条件更新手段と、更新後ライセンス情報生成手段と、暗号化手段と、書き換え手段とを設けたため、コンテンツの再生に応じてコンテンツ利用条件が変化する場合でも、コンテンツ利用条件を更新することができ、正しいコンテンツ利用条件を保持することができる。

【 0 1 5 4 】

この発明のさらにもう 1 つの局面に従ったライセンス発行方法は、利用者が希望するコンテンツのライセンス情報を、携帯可能な独立したハードウェアであるライセンス記憶装置に書き込む。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、さまざまな形態のコンテンツ再生装置を利用してコンテンツの提供を受けることができる。

【 0 1 5 5 】

この発明のさらにもう 1 つの局面に従ったコンテンツ再生方法は、利用者が携帯するライセンス記憶装置に書き込まれたライセンス情報を用いて暗号化コンテンツを復号し再生する。したがって、利用者は、希望するコンテンツのライセンス情報が書き込まれたライセンス記憶装置を携帯し、さまざまな形態のコンテンツの提供を受けることができる。

【図面の簡単な説明】

【図 1】

この発明の第 1 の実施形態によるコンテンツ提供システムの構成を示す図である。

【図 2】

図 1 に示したメモリカードおよびライセンス発行装置の具体的な構成を示すブロック図である。

【図 3】

コンテンツタイトル、コンテンツ ID、およびコンテンツ復号化鍵が対応づけられたデータベースのデータ構造を示す図である。

【図 4】

図 2 に示したライセンス発行装置によるライセンス情報の発行の手順を示すフローチャートである。

【図 5】

メモリカードのライセンス記憶手段に記憶される情報を示す図である。

【図 6】

メモリカードとライセンス発行装置との間での相互認証の手順を示すフローチャートである。

【図 7】

図 1 に示したメモリカードおよびコンテンツ再生装置の具体的な構成を示すブロック図である。

【図 8】

図 7 に示したコンテンツ再生装置によるコンテンツの再生の手順を示すフローチャートである。

【図 9】

この発明の第 2 の実施形態によるコンテンツ再生装置の構成を示すブロック図である。

【図 1 0】

図 1 に示したコンテンツ提供システムの適用例を示す図である。

【符号の説明】

- 1 0 0 メモリカード
- 1 2 0 相手装置認証手段
- 1 3 0 ライセンス記憶手段
- 2 0 0, 2 0 0 a, 2 0 0 b ライセンス発行装置
- 2 1 0 メモリカード認証手段
- 2 5 0, 9 2 0 連結手段

2 6 0, 9 3 0 暗号化手段

3 0 0, 9 0 0, 3 0 0 a, 3 0 0 b コンテンツ再生装置

3 1 0 復号手段

3 4 0 再生手段

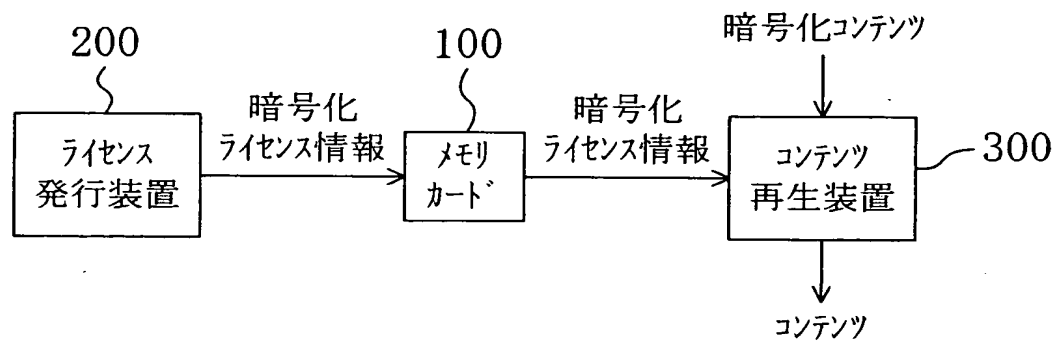
3 5 0, 3 5 0 a, 3 5 0 b 暗号化コンテンツデータベース

9 1 0 コンテンツ利用条件更新手段

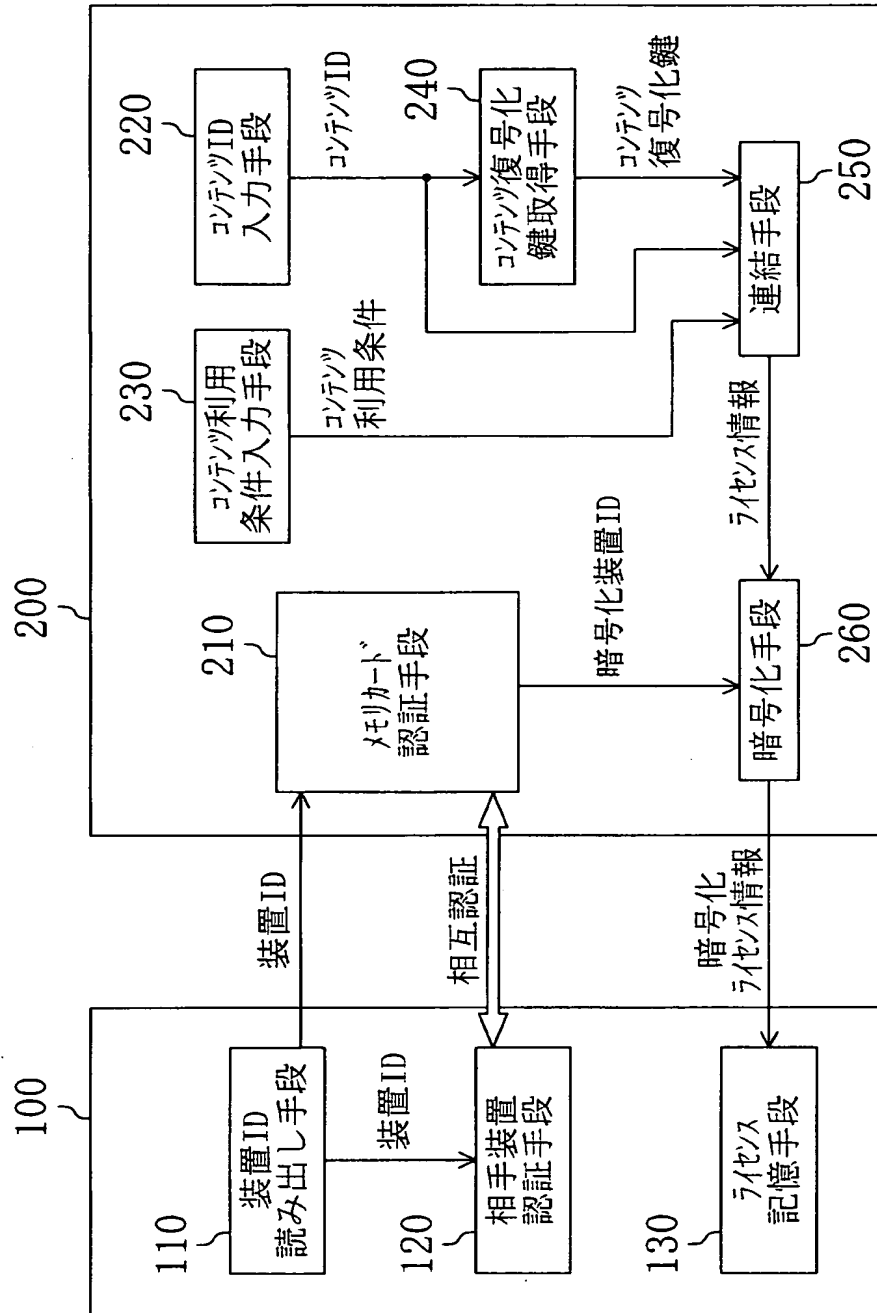
9 4 0 暗号化ライセンス情報更新手段

【書類名】 図面

【図1】



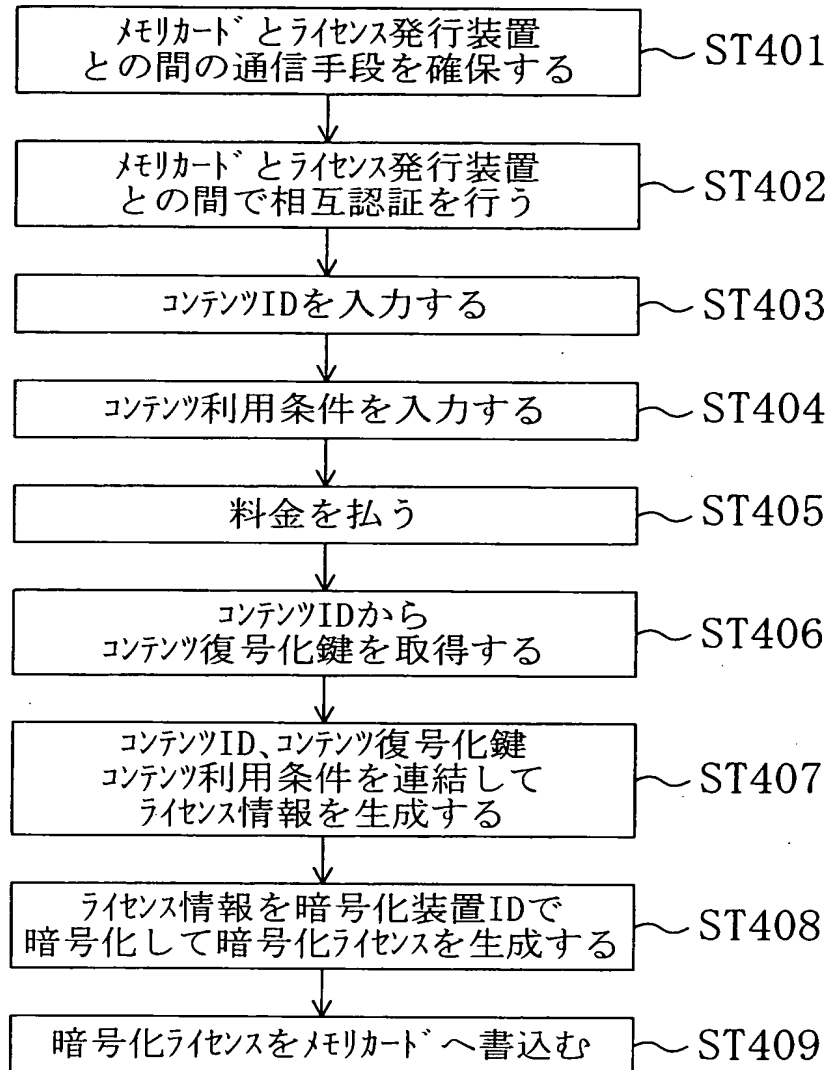
【図2】



【図 3】

31 }	32 }	33 }
音楽1	0001	SSSS1
音楽2	0002	TTTT2
映画1	0003	UUUU3
映画2	0004	VVVV4
:	:	:

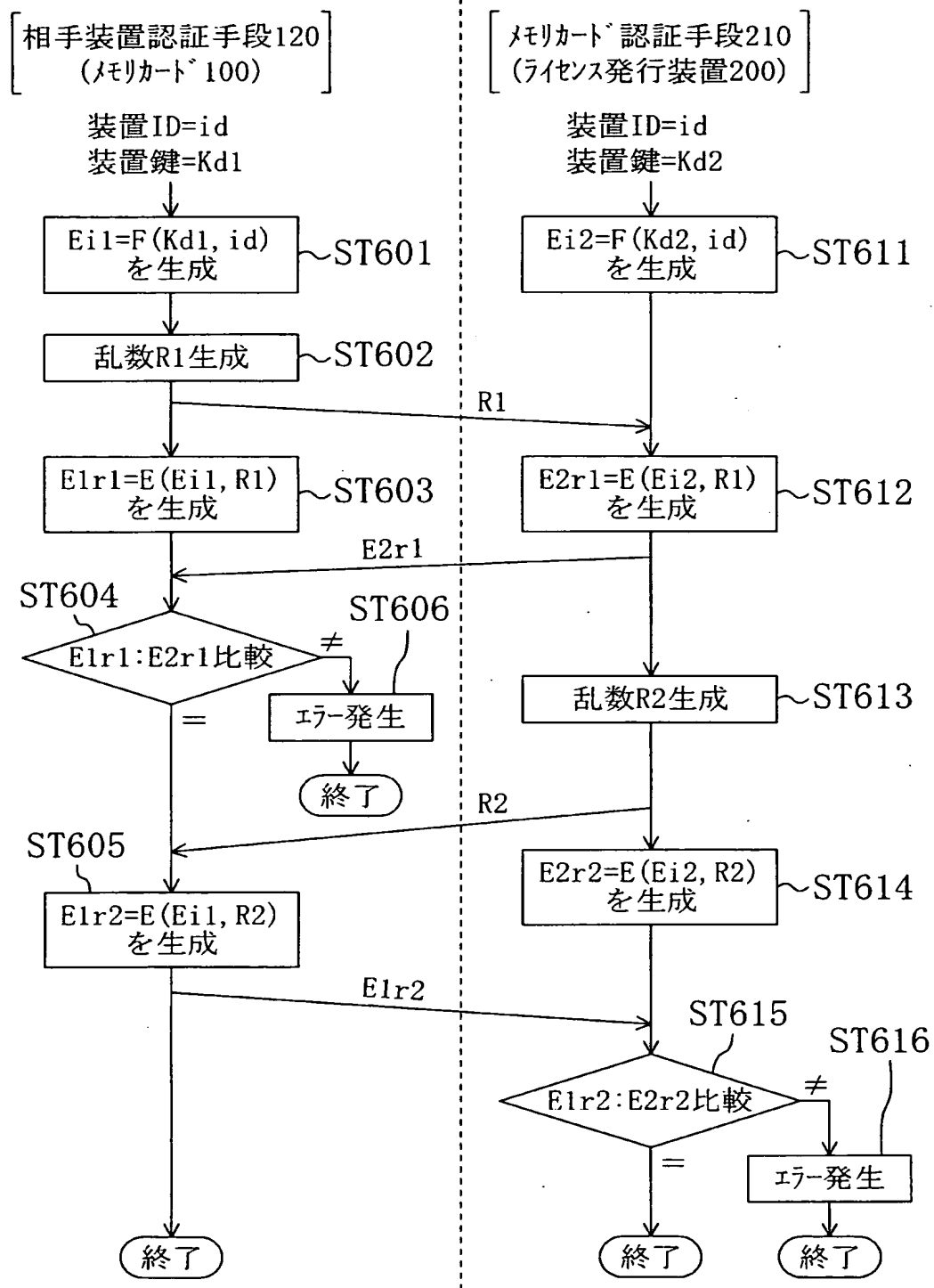
【図 4】



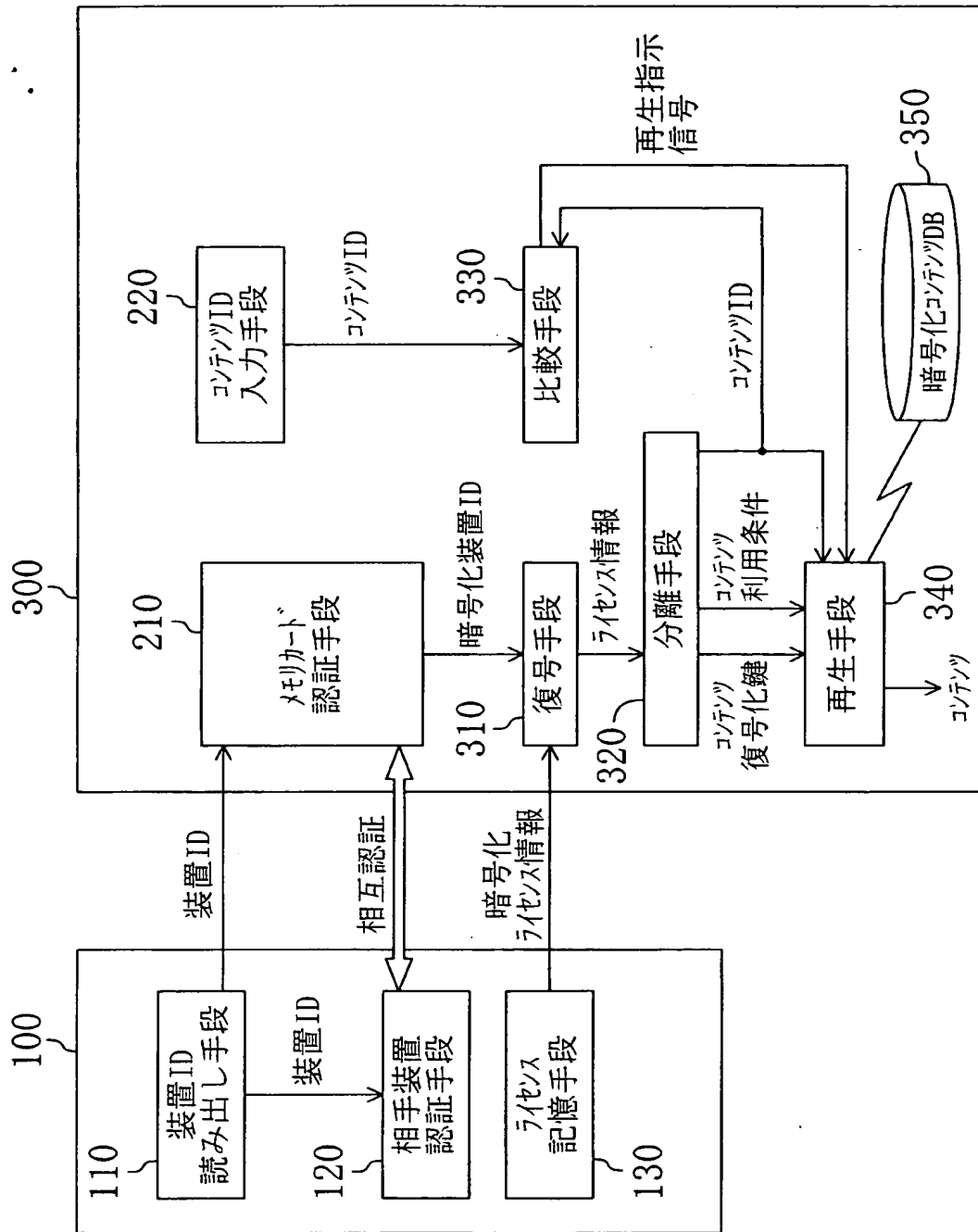
【図 5】

51 }	52 }	53 }
音楽A	歌手1	XXABCD
音楽B	歌手2	XXEFGH
映画A	俳優1	XXJKLM
:	:	:

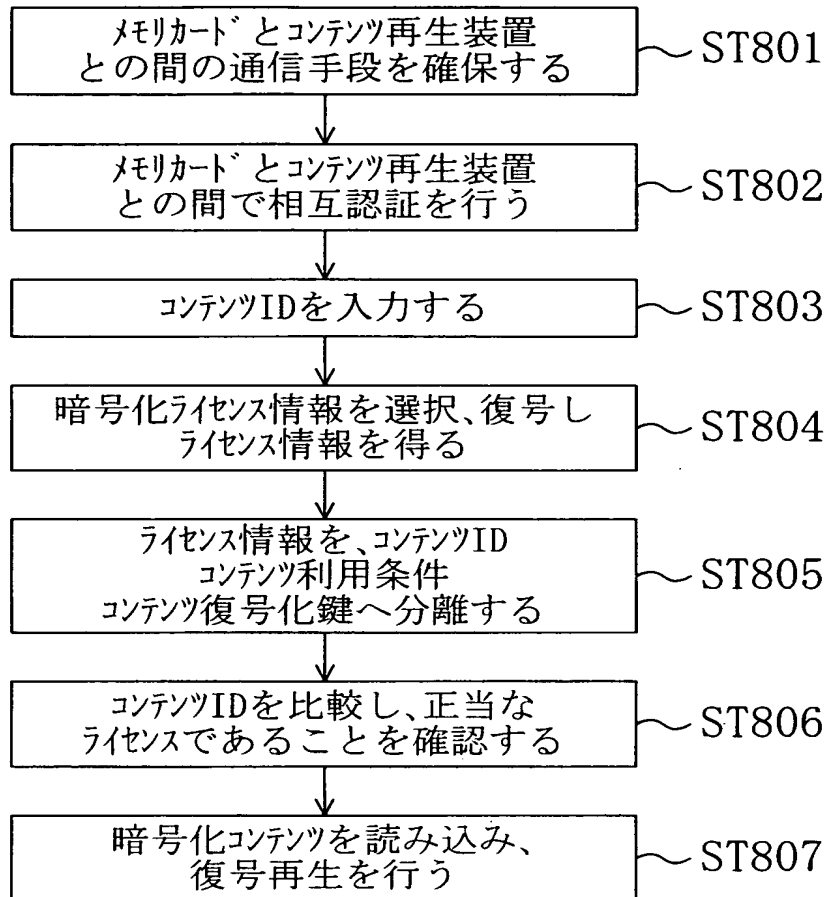
【図6】



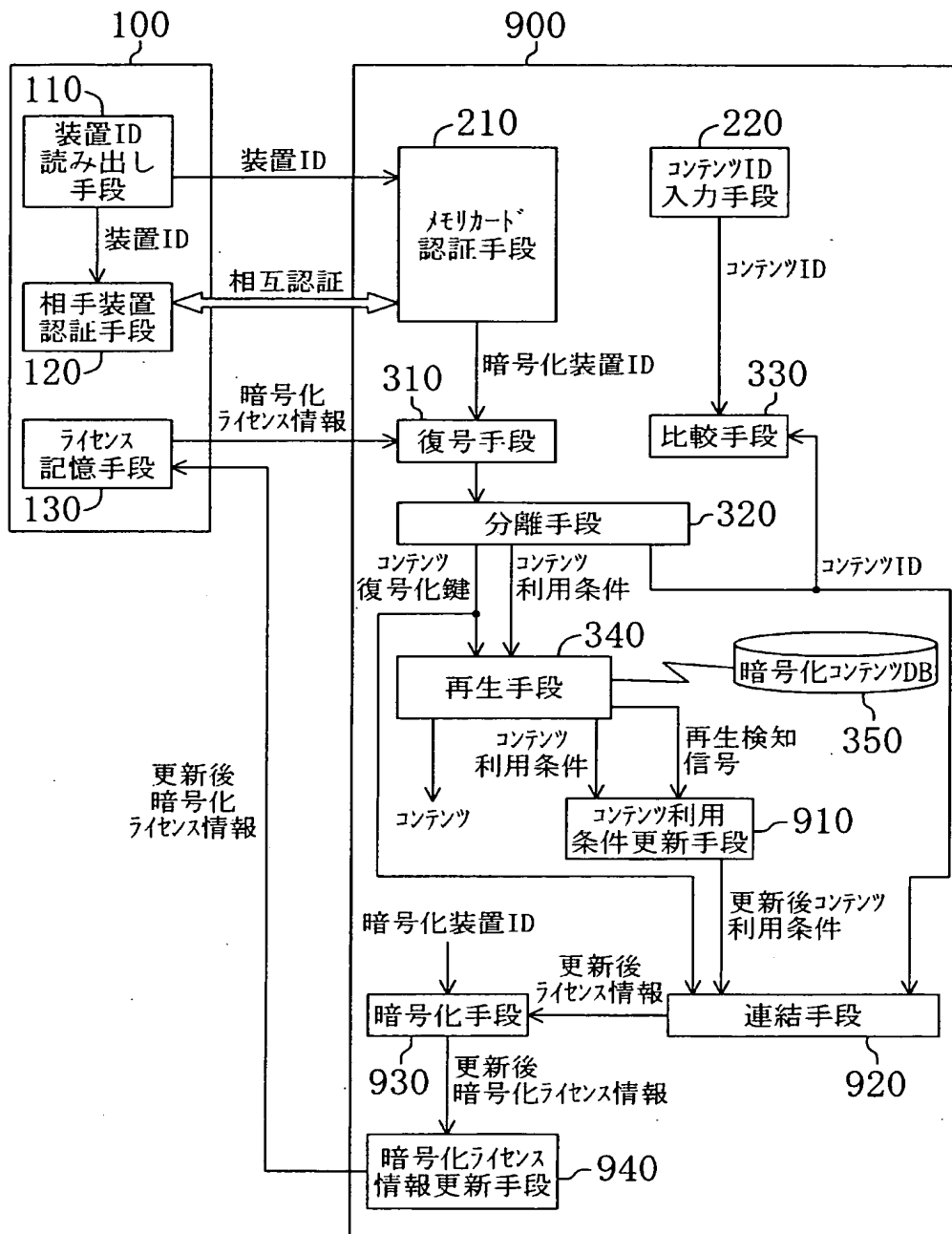
【図7】



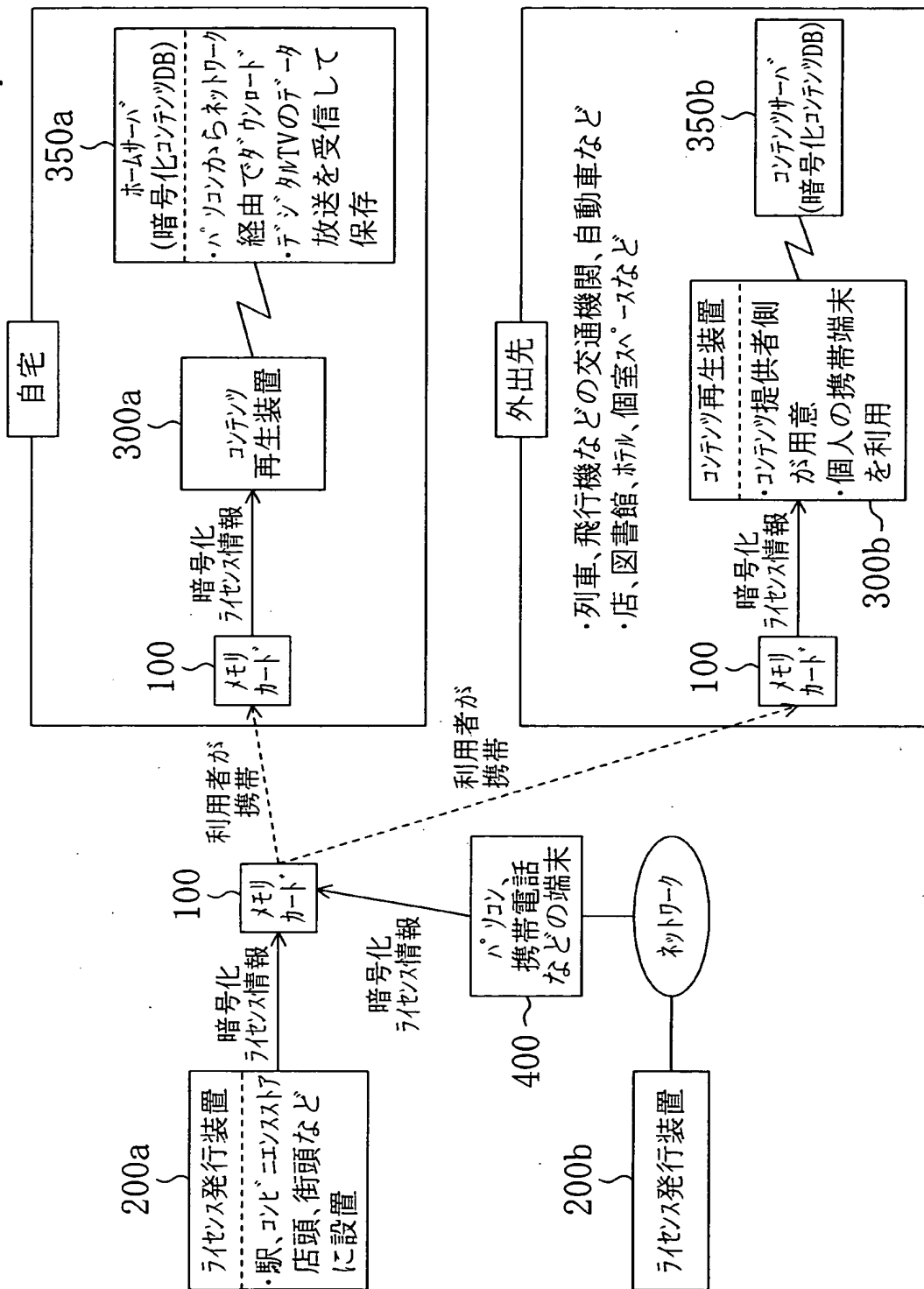
【図 8】



【図9】



【図10】



【書類名】 要約書

【要約】

【課題】 再生装置に限定されずにコンテンツを利用できるようにする。

【解決手段】 ライセンス発行装置 2 0 0 は、利用者が希望するコンテンツのライセンス情報を、利用者が携帯するメモリカード 1 0 0 の装置 I D を用いて暗号化して、当該メモリカード 1 0 0 に書き込む。コンテンツ再生装置 3 0 0 は、利用者が携帯するメモリカード 1 0 0 に書き込まれたライセンス情報を、当該メモリカード 1 0 0 の装置 I D を用いて復号する。そして、コンテンツ再生装置 3 0 0 は、復号したライセンス情報において利用を許可されているコンテンツに対応する暗号化コンテンツを復号して再生する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社